EXHIBIT A

AFFIDAVIT

State of WASHINGTON)
) ss
County of KING)

I, Chris Hansen, being duly sworn, depose and state as follows:

A. Agent Background

1. I have been a commissioned officer with the Seattle Police Department ("SPD") since June, 2000. Since April, 2006, I have served as a Detective in the Fraud, Forgery and Financial Exploitation ("FFFE") Unit, SPD. In addition to annual SPD training regarding local case law developments, I have received specialized training, since my assignment to the FFFE Unit, in the investigation of theft and identity theft, forgery, credit card fraud, mortgage fraud, and online auction fraud. I have also received training on drug interdiction and local seizure/forfeiture laws.

While assigned to the FFFE unit, I have conducted investigations involving forgery, theft, possession of stolen property, credit card fraud, Internet fraud, embezzlement, securities fraud, insurance fraud and identity theft. During this same period, I have applied for and executed numerous search warrants related to fraud investigations.

2. In August, 2008, I became a part-time member of the United States Secret Service Electronic Crimes Task Force, Seattle Field Office, United States Secret Service ("USSS"). Since March, 2010, I have been assigned as a full time member of the USSS E-Crimes Task Force. I hold a Special Deputation appointment through the United States Marshals Service that permits me to seek and execute search warrants supporting a federal task force. As a member of the Seattle USSS E-Crimes Task Force, I investigate violations of federal law in the state of Washington that fall under the responsibility of the

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

USSS, with an emphasis on crimes involving computers, the Internet, and electronic communications. I have received specialized training through the USSS in these areas, as well as in the areas of computer forensics, computer hardware, computer software, network intrusion and electronic crimes.

B. Civil Forfeiture Requested

3. I make this affidavit in support of a Complaint for Civil Forfeiture, pursuant to Title 18, United States Code, Section 981(a)(1)(C), to forfeit to the United States of America:

a. A 1988 black Mercedes Benz automobile, model 300E, four door sedan, identified by VIN #WDBEA30D3JA688786, License Plate #2380LEM (hereinafter "DEFENDANT VEHICLE").

The DEFENDANT VEHICLE is currently registered in the State of Washington to Chantelle Victor, at Seattle, Washington.

4. As set forth below, the DEFENDANT VEHICLE is property derived from proceeds traceable to the crimes of Computer Fraud and Abuse, Wire Fraud, Identify Fraud, and Aggravated Identity Theft, in violation, respectively, of Title 18, United States Code, Sections 1030(a)(4) and (a)(5)(A), 1343, 1028(a)(7), and 1028(A), and also was used to facilitate the commission of the listed crimes.

C. Sources of Information

5. The information contained in this affidavit is based upon my personal knowledge and observations, my training and experience, information provided to me by other law enforcement officers and employees, and a review of documents and records. Because this affidavit is made for the limited purpose of seeking civil forfeiture of a vehicle, I have not set forth every fact I know concerning this investigation. Rather, I have stated only those facts I believe necessary to establish probable cause that the DEFENDANT VEHICLE was used to facilitate, and also is property derived from proceeds traceable to the crimes of Computer Fraud and Abuse, Wire Fraud, Identify Fraud, and Aggravated Identity Theft, in violation, respectively, of Title 18, United States Code, Sections 1030(a)(4) and (a)(5)(A), 1343, 1028(a)(7), and 1028(A).

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

D. The "WEP Hacking" Investigation

6. As part of my duties as a Detective, SPD, and subsequently, as a member of the USSS E-Crimes Task Force, I have been involved in a months-long investigation of a pattern of similar and apparently related computer network intrusions in the Puget Sound region. A number of area small and medium-sized businesses have been targeted in these network intrusions, which have also involved a pattern of theft of financial and personal identifying information (such as credit card account information).

7. Based on the investigation to date, I believe that these network intrusion incidents are the work of a loosely associated group of criminals in the Seattle area, whose relationship has been documented in police reports dating back to May, 2006. Several suspects have been identified, including John E. Griffin, who was the registered owner of the DEFENDANT VEHICLE at the time of the vehicle's impound. Because the businesses that have been victimized in these network intrusion attacks commonly use Wired Equivalent Privacy ("WEP") protection for data security, and this protection has been compromised or "hacked" as part of the intrusion, this investigation has come to be known as the "WEP hacking investigation."

8. Through training and experience, I have learned that suspects who hack wireless networks commonly engage in an activity called, "wardriving." Wardriving is the logging and mapping of the existence of wireless access points. Often this term has been used interchangeably with the term "piggybacking," which is the unauthorized access of a wireless network. The term "wardriving" most appropriately describes only the mapping of access points, while "piggybacking" describes the unauthorized access of a wireless access point.

9. Wardriving involves the use of a car as transportation, a laptop or PDA to run software capable of identifying characteristics of detected wireless networks, a wireless antenna attached to the laptop or PDA for receipt/transfer of wireless RF signals, a data storage device for capturing data from the wardriving activity, and a power source for the laptop.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

10. During the course of investigation, some commonalities emerged which led investigators to believe that suspects were engaging in wardriving and piggybacking activity with the motive being theft and unlawful use of financial information and personal identifying information.

E. DEFENDANT VEHICLE's association with WEP Hacking suspect, JOHN E. GRIFFIN.

11. During the course of this investigation, many individual details of specific hacking and financial fraud incidents led investigators to believe that John E. Griffin was a significant participant in the network intrusion and fraud activity that had been reported to law enforcement by local businesses.

12. While conducting surveillance of targets in this investigation, investigators observed John E. Griffin ("Griffin") driving a Black 1988 Mercedes 300E four door sedan, bearing Washington State license plate number 246ZRI - the DEFENDANT VEHICLE - on a few different occasions. During the period of surveillance, no one else besides Griffin was observed driving or occupying the DEFENDANT VEHICLE. A records check showed the DEFENDANT VEHICLE was registered to Griffin and the mailing address for the registration was the home of Griffin's mother, Vicky Heeley, 7125 176 St SW, Edmonds, WA 98026.

F. Arrest of John E. Griffin for attempt to pass stolen gift cards

13. On October 5, 2010, I learned that Detective (Det.) Hoover of the Bellevue Police Department had been notified that gift cards reported stolen in a Bellevue burglary had been used at a Seattle merchant, The Local Vine. I learned, further, that Det. Hoover believed that the particular burglary involving those stolen gift cards was one of a related series of burglaries, commonly known to local law enforcement as the "Knox Box[1]"

---

[1]A Knox Box is a locked box affixed near the main entrance of a business complex that contains master keys for the business complex for emergency access by firefighters. In what appeared to be a related series of burglaries in Bellevue, WA, the perpetrators had broken into Knox Boxes to access the master keys for buildings that were then burglarized. Suspects had been identified as including Brad Lowe and Joshua Witt, who were also among those identified as suspects in the WEP hacking case. As part of my

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

series. Det. Hoover provided me with a physical description of the suspect who had passed the stolen gift cards at The Local Vine, which description resembled that of Griffin. Since Griffin was a suspect in my WEP hacking investigation, I placed a flag on the address of The Local Vine, which would trigger a notice to me and to Det. Hoover if The Local Vine store owners subsequently contacted law enforcement.

14. On October 21, 2010, Det. Hoover was contacted by NORCOM and told that the Seattle Police had arrested a subject at The Local Vine for using stolen gift cards.

15. Det. Hoover contacted Officer (Off.) Schoenberg at the East Precinct, SPD, who told Det. Hoover that SPD had received a call about a subject using stolen gift cards at The Local Vine. Off. Schoenberg said that when they arrived the bartender pointed to a subject who they identified as John E. Griffin, DOB xx-xx-1975 (Griffin). Off. Schoenberg said they read Griffin the Miranda rights and Griffin told them that he bought the gift cards from Craigslist. Off. Schoenberg said that officers confirmed that the cards were stolen, arrested Griffin, and transported him to the East Precinct (Seattle case 10-368758).

16. Off. Schoenberg gave Det. Hoover two gift cards, with last four numbers of 0618 and 0619 (SRH-2) and six receipts (SRH-3) that he said were given to him by the manager of The Local Vine.

17. Det. Hoover contacted Griffin in an interview room at the East Precinct and confirmed he had received and understood the Miranda rights. Det. Hoover asked Griffin about the gift cards and Griffin told Det. Hoover that he had purchased them from a person advertising through Craigslist about five weeks earlier. Griffin said he saw the ad and responded to the ad through the Craigslist e-mail. Griffin said a subject called him and asked him to meet at the Northgate Mall. Griffin said that he called the guy back a couple times while he was waiting at the Mall and the guy's phone number should be in his phone. Griffin said he bought 12 $50 gift cards from the guy. He said the guy had a

---

investigation of the WEP hacking case, I learned that there were connections and relationships between Lowe, Witt, and Griffin.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

scanner and swiped several of the cards to show that they had $50 on them. Griffin said that after he bought the cards, he tried calling the guy again asking if he had any other gift cards, but the guy never called him back. Det. Hoover asked Griffin if he had any more of the gift cards and he said no, that he had used them all.

18. Det. Hoover asked Griffin what kind of car he (Griffin) drove. Griffin said a black Mercedes, but that it was currently broken down in Renton.

19. On October 21, 2010, I also received notice of the stolen gift card incident at The Local Vine, and also responded to the East Precinct. Since I was familiar with Griffin's car (the DEFENDANT VEHICLE) from my WEP hacking investigation, I asked Patrol to look for Griffin's car in the vicinity of The Local Vine. It was found, and I seized the DEFENDANT VEHICLE and impounded it to the Seattle Police Department's processing room; a secure, access-controlled facility.

20. Meanwhile, Off. Schoenberg transported Griffin to the Bellevue Police Dept. At Bellevue Booking Det. Hoover told Griffin that he knew that Griffin was lying to him about buying the gift cards off of Craigslist. Det. Hoover told him that he knew something about the burglary where the gift cards were taken. Griffin said, "I know, but I can't tell you about it." Griffin told Det. Hoover that he wanted to tell him all about it, but couldn't.

21. Det. Hoover asked Griffin if he was scared of using a stolen gift card. Griffin said that he didn't actually know they were stolen. Det. Hoover told him that the Patrol Officer said that Griffin was nervous and tried to leave the wine bar as soon as the officers walked in. Griffin said that when you use something that someone gave you for free, you get nervous. He said that he was getting a "strange vibe" from the people at the restaurant.

22. The following day, I responded to the Seattle Police Department processing room and viewed the DEFENDANT VEHICLE. Looking into it from the outside, without opening the doors, I was able to see the following articles in open view inside the vehicle:

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

In open view in the passenger seat:

- Laptop, which appeared to be plugged into the cigarette lighter for power, with a USB device (possibly an aircard) plugged into the back of the computer. There was another USB port occupied in the computer, which might be attached to the antenna described below:
    - An antenna, which appears to be a WiFi range booster antenna;
    - Binoculars; and,
    - Large black handset, possibly a phone.

In open view in the center console:

- Cellular data phone.

In open view in the driver door handle:

- A card that appears to be a Washington State Drivers' License.

In open view in the front passenger door:

- CDs/DVDs (unknown whether for music or computer programs).

In open view in the back passenger compartment:

- Box of RAM cards;
- MST Software "Real Time Pricing;" and,
- CD or DVD.

G. Search Warrant MJ10-489 obtained and executed on DEFENDANT VEHICLE

23. On November 26, 2010, a search warrant was signed by the Honorable Magistrate Judge Mary Alice Thieler, authorizing the search of the DEFENDANT VEHICLE and its contents.

24. I subsequently executed that warrant, and in doing so discovered the following:

25. I discovered Griffin's driver's license resting in the interior handle of the driver door. The placement indicates he intentionally left it behind in the DEFENDANT VEHICLE when he had gone into the Local Vine to negotiate the stolen gift cards.

\\

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

26. Upon opening the DEFENDANT VEHICLE, I immediately observed the laptop in the front passenger compartment of the vehicle, with the following items attached:

- Magic Jack USB adapter connecting a phone to the rear of the laptop. Magic Jack enables a user to communicate by phone over an internet connection;
- Hawking Pwr Lnk wireless adapter, attached by USB cable to the side of the laptop. This enables a computer user to access a wireless access point via a strong and stable connection;
- A USB thumbdrive with unknown contents (This device has not yet undergone forensic examination); and,
- A Wagan Tech 150watt AC Power Inverter. This device allows a computer user to connect their laptop to the car's battery via the vehicle's DC power outlet, which lengthens computing time considerably.

27. Continuing the search of the DEFENDANT VEHICLE, I noticed that there was a mount attached to the base of the front passenger seat. This appears to be a mount for a laptop stand, which would allow a person sitting in the driver's seat to access a laptop from a comfortable position, without interfering with the driver's access to the steering wheel or gear shifter. Among the fraudulent purchases under investigation in this case is a laptop stand for a vehicle. Although the component affixed to the base of the front passenger seat of this vehicle appears to be different from components in the fraudulently purchased laptop stand that has been described to investigators, it is a component to which a laptop stand could be attached and it is my belief that this is what the component was installed to support.

28. I also found some cables under the passenger floorboards. I was unable to follow the cables to their terminating connection, but the coaxial cable that I found appears to be the kind that could be used to connect a directional antenna to the Hawking wireless adapter on the laptop, which would allow the user to access wireless access points from a greater distance than normal. It is also possible that this cable is a component of the audio system in the DEFENDANT VEHICLE.

\\

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

29. In the back seat of the DEFENDANT VEHICLE, I found a Cables-To-Go brand case containing tools and materials for assembling networking cables. I researched the contents of the case and discovered that the case partly consisted of tools from a Cables-To-Go Field Service Engineer Kit, which includes tools for customizing and testing networking cables. The case also consisted of couplings from a Cables-To-Go 40-piece RF Adapter Kit, which includes among other pieces, a UHF coupling that could be used to connect the coaxial cable in the front passenger floorboards to the wireless adapter that was attached to the laptop.

30. Det. Dave Dunn, SPD, who is also a member of the USSS E-Crimes Task Force and a certified computer forensic examiner, conducted a forensic examination of the laptop found in the front seat of the DEFENDANT VEHICLE and found it contained hacking tools and other evidence related to specific incidents of network intrusion activity. Other tools, devices, attachments, materials and hand-made components found throughout the DEFENDANT VEHICLE were items that could be used to facilitate the criminal activity under investigation, including a certain device that appears to be a long-range directional antenna that is designed to be mounted on a pole at a fixed location and attached to a computer.

31. I observed that all the windows of the DEFENDANT VEHICLE, except the front window, had limo-tint on them. A person conducting criminal activity from inside the DEFENDANT VEHICLE (such as network intrusions for the purpose of stealing personal identifying information, user credentials, and financial data) would be able to do this activity in nearly complete privacy. It would be nearly impossible for any person to observe the activity occurring inside the DEFENDANT VEHICLE from a short distance away. Not only were the windows heavily tinted, but there were also blinds attached to the rear passenger compartment windows that further obscured the interior of the DEFENDANT VEHICLE. The DEFENDANT VEHICLE did not have such tinting on the windows when investigators first photographed it in the suspects' possession in February, 2010.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

32. Other items found inside the car included packing slips for items sent to drop-addresses used by the suspects for shipments of fraudulent purchases. In addition to the packing slips there was merchandise in the DEFENDANT VEHICLE that matched the items fraudulently purchased from the automotive companies referenced in paragraph 33, below. This demonstrated that the suspects were using the DEFENDANT VEHICLE for retrieving and transporting fraudulent purchases.

33. In addition, while inspecting the DEFENDANT VEHICLE, I found that it contained numerous automotive parts purchased by means of stolen financial information. During the course of this investigation, one victim automotive business reported a total loss of approximately $1,970.80 related to parts fraudulently purchased for a 1988 Mercedes Benz 300E. The same business reported a total loss of approximately $901.71 related to parts fraudulently purchased for 1989-1992 Mercedes Benz 300E vehicles, and I received information that these parts could be used for a 1988 Mercedes Benz 300E. In addition, another business reported a $846.96 loss on a set of four tires that were delivered to the targets in this investigation while they were under surveillance. The targets then mounted these tires onto the DEFENDANT VEHICLE. Yet another automotive business reported a total of approximately $11,381.13 in fraudulent transactions related to the conspiracy, not including shipping or taxes. I discovered during the course of investigation that eleven of the transactions, totaling approximately $4722.85, were conducted using credit card numbers that suspects stole via network intrusion from a victim business identified in the WEP investigation. Included among the fraudulent transactions reported by the second automotive business are a number of transactions consisting of auto parts that could be used on the DEFENDANT VEHICLE. Parts on the DEFENDANT VEHICLE that appeared to have very little wear appeared to match parts that were fraudulently purchased from these victim businesses. Therefore, the vehicle itself is both evidence of the crimes under investigation, and constitutes proceeds of the same.

\\

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

34. Additionally, the DEFENDANT VEHICLE contained mail, reference materials for navigating computer systems, notebooks containing stolen personal identifying information and stolen user credentials, and one or more access devices opened in the name of identity theft victims. The DEFENDANT VEHICLE was thus being used as a storage locker for contraband and materials designed to carry out network intrusion activity and identity theft, and was also facilitating the criminal activities of Computer Fraud and Abuse, Identity Theft and Wire Fraud, in this way.

35. Based on my training and experience, I know that people who engage in the types of criminal conduct that I am investigating in this case typically use automobiles, and also the types of digital devices that I have observed in the DEFENDANT VEHICLE to commit those crimes. It has been my experience that it is common for persons engaged in network intrusion activity for theft of personal identifying information and financial information to use digital devices (including computers, mobile or cellular telephones and other cellular devices capable of data transfer over the internet, such as Blackberries), electronic storage devices and other digital hardware (such as air-cards, wifi booster antennas and bluetooth devices), as a tool or instrumentality in committing that criminal activity. In particular, vehicles are used to transport suspects to within proximity of electronic networks they wish to target for network intrusion activity. Wifi booster antennas enable suspects to access distant electronic networks, resulting in lower risk of detection during wardriving and/or piggybacking. Once a suspect has gained unauthorized access to a wireless network, computers in the vehicle can be used to run programs such as port scanning software and password recovery software designed to breach security on machines within the network; and to save stolen personal identifying information, stolen financial information, stolen user credentials and many other types of data that can be harvested from a breached electronic network.

\\

\\

\\

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

H. Conclusion

36. For the reasons stated above, there is probable cause to believe that the DEFENDANT VEHICLE is property derived from proceeds traceable to the crimes of Computer Fraud and Abuse, Wire Fraud, Identify Fraud, and Aggravated Identity Theft, in violation, respectively, of Title 18, United States Code, Sections 1030(a)(4) and (a)(5)(A), 1343, 1028(a)(7), and 1028(A), and also was used to facilitate the commission of the listed crimes.

As such, the DEFENDANT VEHICLE, a 1988 black Mercedes Benz automobile, model 300E, four door sedan, identified by VIN# WDBEA30D3JA688786, is subject to forfeiture to the United States pursuant to Tile 18, United States Code, Section 981(a)(1)(C).

Dated this 13 day of April, 2011.

CHRIS HANSEN, Affiant
Task Force Officer
United States Secret Service

VERIFICATION OF AFFIDAVIT

SUBSCRIBED and SWORN to before me this 13th day of April, 2011, by Chris Hansen.

MEGAN SEABORN
STATE OF WASHINGTON
NOTARY PUBLIC
MY COMMISSION EXPIRES
05-23-14

Print: Megan Seaborn
Notary Public in and for the
State of Washington, residing
at Seattle, WA
Expires: 5/23/14

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970